FORTRA

DATASHEET (FORTRA BRAND PROTECTION)

Compromised Credentials Monitoring

Use of stolen credentials leads the way in tactics used by threat actors. Compromised credentials pose a serious threat to organizations, leading to data breaches, reputational harm, and account takeovers. While monitoring for these risks is essential, it often comes with significant challenges. Limited visibility, restricted access, and knowledge gaps can allow threat actors to stay one step ahead.

Fortra Brand Protection provides the ability to quickly respond and implement countermeasures to guard against attacks. Our Compromised Credentials Monitoring delivers broad visibility into stolen employee and customer credentials revealed from dark web sites and harvested from third-party leaks, infostealers, botnets, and other forms of malware. The enhanced visibility allows organizations to quickly respond and implement countermeasures, such as forced password resets and lockouts to guard against potential account takeovers, breaches, and malware attacks.

Compromised Credentials Monitoring Capabilities

Expose Threats Quickly

Enhance the detection of compromised credentials on dark web forums, websites, and blogs, as well as compromises caused by third-party leaks, botnets, infostealers, and other malware.

Expert Curation

Fortra Brand Protection's team of dark web analysts refine incident search results provided by external feeds and internal proprietary technology to quickly separate relevant threats from the noise.

Protect Employees and Customers

Detect both employee and customer compromised credentials for sale, whether leaked internally or stolen by threat actors.

Exclusive Insights

Gain access to rich credential data that is fully actionable and not protected behind paywalls.

Proactively Defend

Guard against potential attacks by implementing countermeasures designed to protect your organization's brand, employees, and customers through forced password resets, account lockouts, and by stopping the exfiltration of outbound transfers in-flight.

PRODUCT SUMMARY

Fortra Brand Protection's Compromised Credentials Monitoring provides broad visibility into actionable employee and customer stolen credentials uncovered from the dark web and harvested through malware, to proactively guard against future attacks.

Organizations can expose threats quickly through enhanced detection of compromised credentials caused by:

- Third-party leaks
- Infostealers
- Botnets
- And other malware

The enhanced visibility provides the ability to quickly respond and implement countermeasures, such as:

- Forced password resets
- Account lockouts
- Stop the exfiltration of outbound transfers in-flight

Comprehensive Protection Against Dark Web Threats

Uncover brand threats and compromised credentials across anonymized dark web sites and malware with Fortra Brand Protection's Dark Web Monitoring, and Compromised Credentials Monitoring.

Dark Web Monitoring

Dark sites, marketplaces, and forums

Compromised Credentials Monitoring

Infostealers, botnets, and other malware

Brand and executive mentions, stolen PII BINS, phishing kits, emails, card data, fraud tools, initial access brokers

Actionable compomised logins
Emails, passwords, secret codes
Not parked behind paywalls

Continuous targeted surveillance
Monitor for changes in activity

Implement proactive countermeasures
Forced password resets/account lockouts
Stop exfiltration of outbound tranfers

Find out more at **Fortra.com**

FORTRA

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.